COOLEY LLP
MICHAEL G. RHODES (116127) (rhodesmg@cooley.com)
KYLE C. WONG (224021) (kwong@cooley.com)
AARTI G. REDDY (274889) (areddy@cooley.com)
101 California Street, 5th Floor
San Francisco, CA 94111-5800
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

CHARLES A. WOOD (310702) (cwood@cooley.com)
1299 Pennsylvania Ave., NW, Suite 700
Washington, DC 20004
Telephone: (202) 842-7800
Facsimile: (202) 842-7899

Attorneys for Defendant
NOOM, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

AUDRA GRAHAM and STACY MOISE, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

NOOM, INC. and FULLSTORY, INC.,

Defendants.

Case No. 3:20-cv-06903-LB

DEFENDANT NOOM, INC.'S REPLY IN SUPPORT OF ITS MOTION TO DISMISS PLAINTIFFS' FIRST AMENDED CLASS ACTION COMPLAINT

Hearing Date: April 8, 2021
Hearing Time: 9:30 a.m.
Judge: Honorable Laurel Beeler

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

Statutes

TABLE OF AUTHORITIES
(continued)

Page

Other Authorities

I. INTRODUCTION.

Plaintiffs Graham and Moise admit in their Opposition ("Opposition" or "Opp.") that they had no reasonable expectation of privacy from Defendant Noom, Inc. ("Noom") with respect to any data Plaintiffs submitted through Noom's website when signing up for Noom's weight loss program. Plaintiffs nevertheless claim that Noom engaged in criminal wiretapping by permitting its service provider FullStory, Inc. ("FullStory") to collect that data on Noom's behalf. Yet Plaintiffs fail to allege this data was ever sold, disseminated, or used except to "improve [Noom's] website design and customer experience." (ECF No. 27 ¶ 18 ("FAC").) Similarly absent is any claim by Plaintiffs that this "interception," caused them any injury whatsoever. The facts alleged do not support a claim for relief, and Plaintiffs' Opposition offers not a single argument or legal authority to the contrary.

As to Plaintiffs' California Invasion of Privacy Act ("CIPA") claims, Plaintiffs concede that Noom was a party to the communications, which precludes all theories of liability under Section 631. Plaintiffs then invite this Court to recognize a private right of action under Section 635 in contravention of the clear statutory language of Section 637.2. Plaintiffs also do not explain how FullStory's code is a device "primarily or exclusively designed or intended for eavesdropping," or how Noom's mere possession of FullStory's code caused them any injury. Likewise, Plaintiffs' constitutional claims fail for lack of a reasonable expectation that the data they voluntarily sent to Noom should remain hidden from Noom and its service providers, or that the alleged use of the data would be highly offensive to a reasonable person.

Finally, and contrary to Plaintiffs' claims, opening the litigation floodgates ***is*** a relevant consideration, just as it has been for 110+ years of federal court decisions.[1] Its relevance goes beyond judicial efficiency; a rush to the courthouse is also a bellwether of an unreasonable judicial interpretation of a longstanding statute. The recent frenzy to litigate similar issues presented in this case in almost sixty cases shows that the thinly-reasoned *Revitch* decision on which Plaintiffs premise virtually all of their arguments was just such a bellwether. This Court should decline Plaintiffs' invitation to drastically expand the scope of CIPA and dismiss all of Plaintiffs' claims.

[1] *See* Marin K. Levy, *Judging the Flood of Litigation*, 80 U.Chi. L. Rev. 1007, 1008 n.1 (2013).

To do otherwise will criminalize not just service providers like FullStory, but also the plethora of other hosting services, storage providers, and other tools that form the backbone of the Internet.

II. ARGUMENT.

A. All of Plaintiffs' CIPA Claims Fail.

1. Noom Cannot Have Violated Section 631 Because It Was a Party to the Alleged Communications.

Plaintiffs concede that Section 631 "appl[ies] only to eavesdropping by a third party and not to recording by a participant to a conversation." *Warden v. Kahn*, 99 Cal. App. 3d 805, 811 (1979) (citation omitted); *see also Membrila v. Receivables Performance Mgmt., LLC*, 2010 WL 1407274, at *2 (S.D. Cal. Apr. 6, 2010) (same); *Rogers v. Ulrich*, 52 Cal. App. 3d 894, 899 (1975) ("It is never a secret to one party to a conversation that the other party is listening to the conversation . . . ."). Plaintiffs also concede that because Noom was a party to the underlying communication, Plaintiffs cannot hold Noom directly liable under CIPA. (Opp. at 3 n.2.) Instead, Plaintiffs seek to impose liability on Noom solely based on an aiding and abetting theory—presenting a novel and unfounded argument that the statutory reference to "any person" in Section 631(a) permits the imposition of such liability. This argument fails.

First, Plaintiffs wrongly contend that Noom can be held liable as an aider or abettor based on a reference to "any person" in Section 631. Yet Plaintiffs' position is contrary to the rule that "there is a presumption that a given term is used to mean the same thing throughout a statute." *Brown v. Gardner*, 513 U.S. 115, 118 (1994). The "any person" language on which Plaintiffs rely applies to the entirety of the Section 631 provision, including the clause related to direct liability. Cal. Penal Code ("CPC") Section 631(a) ("***Any person*** who [themselves wiretap] . . . or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable . . . .") (emphasis added). Plaintiffs admit (as they must) that Noom cannot be held directly liable as a "person" under Section 631, yet simultaneously argue that the very same word somehow renders Noom liable under an aiding and abetting theory. This inconsistency is fatal to Plaintiffs' position.

Plaintiffs' argument is also contrary to another canon of statutory interpretation:

"ambiguous penal statutes are construed in favor of defendants . . . [if] two reasonable interpretations of the same provision stand in relative equipoise." *People v. Avery*, 27 Cal. 4th 49, 58 (2002); *see Warden*, 99 Cal. App. 3d at 814, 818 n.3 (observing that as a penal statute, ambiguity in Section 631 should be interpreted narrowly). This principle should be applied here, where Plaintiffs allege no cognizable injury whatsoever, *supra* Section 1, yet seek the severe penalty of $5,000 per alleged CIPA violation. (FAC ¶ 76.) *See People v. Vogel*, 46 Cal. 2d 798, 804 (1956) (holding that statutory construction must align with "good sense and justice").

Second, Plaintiffs' attempt to hold Noom vicariously liable based on an aiding and abetting theory is unsupported by applicable case law. Indeed, aside from *Revitch*, Plaintiffs cite no cases applying aiding and abetting liability under Section 631 to a party to the underlying communication—Plaintiffs instead cite cases with third party defendants. *Compare Revitch v. New Moosejaw, LLC*, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) *with In re Lenovo Adware Litig.*, 2016 WL 6277245 (N.D. Cal. Oct. 27, 2016) (denying motion to dismiss for a defendant that enabled software that intercepted communications between users and third-party websites); *Ribas v. Clark*, 38 Cal. 3d 355, 361-62 (1985) (denying motion to dismiss for an independent third party who listened to a call); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 596, 608 (9th Cir. 2020) ("*In re Facebook III*") (denying motion to dismiss for claim that an "unauthorized third-party['s]" "Like" button intercepted communications between users and third-party websites).

Prior to *Revitch*, the only published case to consider precisely whether parties to communications could be subject aiding and abetting liability under Section 631 correctly held that such liability could not exist. In *Powell v. Union Pacific R.R. Co.*, 864 F. Supp. 2d 949 (E.D. Cal. 2012), the plaintiff alleged that a union officer eavesdropped on a phone call with his former union supervisor. He later asserted aiding and abetting claims against his former supervisor, who was a party to the communication and permitted the alleged eavesdropping. *Id.* at 954. The plaintiff in *Powell* "contend[ed] that the language of section 631 is clear and a participant should be liable for aiding or conspiring with a third party to enable that party to listen in on the call." *Id.* Like Noom, the defendant argued that "section 631(a) applies to third party actions and therefore, as a party to the call, he cannot be liable as a matter of law." *Id.* Carefully surveying longstanding precedent,

the court agreed with defendant, stating as follows:

> Section 631 was aimed at one aspect of the privacy problem—eavesdropping, or the secret monitoring of conversations by third parties. . . . . The third party focus of section 631 is confirmed by *Rogers v. Ulrich*, 52 Cal.App.3d 894, 125 Cal.Rptr. 306 (1975), where the court held that only a third party could violate the section 631 proscription on eavesdropping. . . . Given the settled nature of the third-party focus of section 631, the court declines to adopt plaintiff's alternate reading.

Id. at 955-56 (internal quotation marks and citation omitted). In observing the "third party focus" of Section 631 the *Powell* court examined years of CIPA precedent that Plaintiffs fail to distinguish.

Instead, Plaintiffs try to distinguish *Powell* by arguing that because the two union employees "were jointly conducting" an investigation, one of them could not be treated as a third party. (Opp. at 5.) This is unpersuasive, as the *Powell* court rejected the exact argument Plaintiffs seek to advance here.[2] Further, contrary to Plaintiffs' claim that the reasoning of *Ribas* supports application aiding and abetting liability on Noom (Opp. at 4), *Ribas* is consistent with Noom's position because the defendant there was a separate party—a third party eavesdropping on a telephone line—and not an intended recipient of the communication between husband and wife. *Supra* Section II(A)(i). And Plaintiffs cannot distinguish *Membrila* and *Rogers* as instances where the plaintiff sought to hold a party to a communication directly liable under CIPA—both cases unequivocally affirm that Section 631 only criminalize eavesdropping by ***third parties***. *Compare* Opp. at 3 n.2 *with Membrila*, 2010 WL 1407274, at *2; *Rogers*, 52 Cal. App. 3d at 897-99. In *Rogers*, the defendant recorded his conversation with plaintiff using "a tape recorder jack [that] had been recently installed on [his] telephone by the telephone company." 52 Cal. App. 3d at 897. The plaintiff there did not assert the defendant aided and abetted wiretapping accomplished by the telephone company based on its provision of tools to record the conversation. Like here, this would be absurd.

The *Powell* court also interprets CIPA in a manner consistent with the federal Wiretap Act, which also exempts from liability a person who is a "party" to the communication. 18 U.S.C. § 2511(2)(c), (d). "Courts perform the same analysis for both the Wiretap Act and CIPA regarding

[2] Plaintiffs also attempt to distinguish *Powell* by arguing that third parties that "were jointly conducting" an investigation are not separate parties under CIPA. (Opp. at 5.) Yet if Plaintiffs contend that persons working towards the same purpose are not separate "persons," then they must concede that FullStory, as Noom's contractor, would not be a separate "person" under Section 631.

the party exemption." *In re Facebook III*, 956 F.3d at 607. That statute also does not allow for ***any*** aiding and abetting liability, and is thus fundamentally inconsistent with the broad construction of aiding and abetting liability under CIPA that Plaintiffs propose here. *Kirch v. Embarq Mgmt. Co.*, 702 F.3d 1245 (10th Cir. 2012). (Opp. at 6.) Plaintiffs simultaneously disclaim the application of the federal Wiretap Act (Opp. at 6) while citing it as support for their arguments elsewhere. (Opp. at 6, 7, 9.) Consistent with *Powell* and the federal Wiretap Act, Section 631 should not be drastically expanded to encompass parties to the communication.

Third, Noom respectfully submits that the case law has not kept current with the advent of new technologies that are now ubiquitously deployed by website operators. In this brief, Noom agrees with the arguments in FullStory's concurrently filed Reply Brief that the implementation of third-party software embedded on a website's software stack does not transform that software into a third party for purposes of CIPA liability. *Javier v. Assurance IQ, LLC*, 2021 WL 940319, at *4 n.5 (N.D. Cal. Mar. 9, 2021) (rejecting argument that defendant's website software was non-party to the communication). Because FullStory was a party to the communication, there was no first party liability for Noom to aid and abet, and Plaintiffs' theory fails for this additional reason.

Finally, as Noom predicted, Plaintiffs rely heavily on *Revitch* and *Facebook* to support their argument that CIPA permits aiding and abetting liability. These arguments are unavailing. To start, *Revitch* does not involve, as Plaintiffs claim, "the same facts and issues presented here." (Opp. at 4.) The plaintiff in *Revitch* alleged that his PII was collected when visiting Moosejaw's website; that this information was shared with third parties; and that these third parties then used that information for their own purposes, including to unmask user identities and send users physical postcards. *Revitch*, 2019 WL 5485330, at *3. Plaintiffs further alleged that the code in question "scanned [plaintiff's] computer for files" that revealed his identity and browsing habits. None of these facts are alleged here, and Plaintiffs only allege that Noom collected user information to "improve their website design and customer experience." (FAC ¶ 18.)

More importantly, although the *Revitch* court denied a motion to dismiss Section 631 aiding and abetting claims against Moosejaw, its analysis is confined to a single paragraph that cites no case law and provides no basis for disagreeing with *Powell*. *Revitch*, 2019 WL 5485330, at *3-4.

The decision also fails to address the overwhelming weight of the case law that makes clear that Section 631 only applies to third parties. Plaintiffs wrongly contend that the court in *Revitch* "followed the California Supreme Court's decision in *Ribas v. Clark*" by holding that a party to a communication could be liable for aiding and abetting under Section 631. (Opp. at 4.) The *Ribas* court did not impose, let alone address, aiding and abetting liability on a party to a communication. *Supra* p. 3-4. Accordingly, this Court should decline to follow *Revitch* and instead adopt the longstanding legal principles and legislative intent recognized in *Powell*.

Plaintiffs also incorrectly argue that the Ninth Circuit "rejected the same argument Noom advances here" in *In re Facebook III*. (Opp. at 4.)[3] Conspicuously absent from their Opposition is any explanation of the facts of that case, which were key to the Ninth Circuit's holding and demonstrate why that decision is wholly inapplicable here. To start, unlike Noom, Facebook was not the intended recipient of the intercepted communication. The Ninth Circuit grappled with a different question altogether: whether a ***non-party*** to the communication could avail itself of the party exception when intercepting GET requests between an individual internet user and various websites. *See In re Facebook III*, 956 F.3d at 589. Facebook installed "cookies [that] allegedly continued to capture information ***after a user logged out of Facebook and visited other websites***." *Id.* at 596 (emphasis added). Analogizing to cases involving defendants who were not intended recipients of similar requests, the court concluded that Facebook was not entitled to immunity under the party exception and could be held liable under CIPA. *Id.* at 607 (citing *United States v. Szymuszkiewicz*, 622 F.3d 701, 703 (7th Cir. 2010) (affirming conviction where defendant employed software that caused employer's email to duplicate and forward all emails)). Extending *In re Facebook III* to hold that even intended recipients of internet communications (that is, user actions on the website that are tracked by that website) can be liable under CIPA would be contrary

[3] Expansion of *In re Facebook III* in the manner that Plaintiffs contemplate is also inadvisable given that the case is recognized by leading experts as a departure from prior decisions and is under consideration for certiorari by the Supreme Court. *See* Venkat Balasubramani, *Ninth Circuit Reinstates Decade-Old Lawsuit Against Facebook For Tracking Logged-Out Users–In re Facebook Internet Tracking*, Tech. & Marketing L. Blog (Apr. 22, 2020), https://blog.ericgoldman.org/archives/2020/04/ninth-circuit-reinstates-decade-old-lawsuit-against-facebook-for-tracking-logged-out-users-in-re-facebook-internet-tracking.htm; *Facebook, Inc. v. Davis*, *petition for cert filed*, (Nov. 20, 2020) (No. 20–727).

to the plain language of that decision and well-established precedent. *Supra* Section II(A)(1).

There is also no merit to Plaintiffs' claim that "[t]he amount of information [Noom] monitor[s] is more extensive here than it was in *In re Facebook III*." (Opp. at 5.) The *In re Facebook III* plaintiffs alleged that "by correlating users' browsing history with users' personal Facebook profiles—profiles that could include a user's employment history and political and religious affiliations—Facebook gained a cradle-to-grave profile without users' consent." *In re Facebook III*, 956 F.3d at 599. By contrast, Plaintiffs here visited Noom's website and voluntarily shared certain unspecified information with Noom (*i.e.*, keystrokes, mouse clicks, and information regarding their weight loss goals) during their sign-up process. (FAC ¶ 2.) There is no allegation that Noom collected any information regarding Plaintiffs' actual use of the app, compiled this information or created any kind of profile; disseminated the information to any third party or used it for any purpose other than routine site maintenance. Rejecting Plaintiffs' attempt to expand the scope of *In Re Facebook III* would not be "reversible error," as Plaintiffs baselessly claim.

2. The Information that Noom Allegedly Intercepted Is Not Content.

Plaintiffs devote three full pages of their Opposition to arguing that Noom intercepted "content" by collecting "mouse clicks," "keystrokes" and "payment card information." (Opp. at 6-8.) Yet nowhere do they dispute that a significant portion of the information they allege Noom unlawfully intercepted—*e.g.*, "the date and time of the visits, the duration of the visits, Plaintiffs' IP addresses, their locations at the time of the visits, their browser types, and the operating systems on their devices" (FAC ¶ 43)—is unambiguously ***not*** content but "record information." *See In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014) (holding that "[c]ustomer record information" such as "name," "address," and "subscriber number or identity" are characteristics of a message rather than content that falls within the ambit of the federal wiretapping act). Plaintiffs' claims should in the least be dismissed as to any record information.

3. Plaintiffs Fail to Plead Statutory and Constitutional Standing in Support of Their Section 635 Claims.

Plaintiffs attempt to avoid dismissal of their Section 635 claim by arguing that they have statutory and constitutional standing to pursue these claims. They are wrong.

Plaintiffs must plead some form of injury to support statutory and constitutional standing for their Section 635 claims. CPC § 637.2(a); *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). As Noom argued in its Motion, Plaintiffs have not pled that Noom's alleged possession of FullStory's code caused them any harm whatsoever. (Mot. at 9-10; FAC ¶ 89.) Plaintiffs' Opposition does not dispute this, and instead claims that the mere allegation of a statutory violation is sufficient to confer standing. (Opp. 8-10.) These arguments fail.

First, as to statutory standing, Plaintiffs claim that they are not required to plead injury because Section 637.2(c) states that "actual damages" "is not a necessary prerequisite" for a CIPA claim. (Opp. at 9.) But Plaintiffs' argument ignores the very first clause of the same statutory provision, which states the exact opposite—*i.e.*, that only persons "injured by a violation of this chapter may bring an action." CPC § 637.2(a). Here, Plaintiffs fail to plead actual damages ***or*** non-economic injury. Plaintiffs generally allege that "Defendants recorded Plaintiffs' electronic communications" (FAC ¶ 2); they had a "reasonable expectation that their PII, PHI, and other data would remain confidential" (*id.* ¶ 89); and that "session recording technologies such as FullStory's ***can*** leave users vulnerable to data leaks and the harm resulting therefrom." (*Id.* ¶ 34 (emphasis added).) Yet nowhere do they claim to have sustained any real or potential injury by Noom's use of FullStory. (*Id.* ¶ 18; Opp. at 10.) As such, Plaintiffs' attempt to conflate "actual damages" and "injury" cannot save their Section 635 claim, which must be dismissed for this reason alone.

Second, Plaintiffs also do not plead injury-in-fact to satisfy constitutional standing. To avoid dismissal, Plaintiffs resort to misconstruing their own allegations, claiming that they "not only allege that Noom possessed a wiretapping device, but also allege Noom's knowledge and active involvement in using that device." (Opp. at 10.) Not so. Plaintiffs merely allege that Noom partnered with FullStory pursuant to an agreement and "deployed" FullStory's software. (FAC ¶¶ 36-40.) In any event, "knowledge and active involvement" in using a wiretapping device is not a basis for liability under Section 635 of CIPA. Section 635 ("manufactures, assembles, sells, offers for sale, advertises for sale, possesses, transports, imports, or furnishes to another any device…").

Plaintiffs also rely heavily on *Revitch* to argue that their allegations are sufficient to confer Article III standing. (Opp. 8-10.) Here again, *Revitch* is both distinguishable and wrongly decided.

In contrast to *Revitch*, Plaintiffs fail to allege any specific injury, as discussed above. *Compare with supra* Section II(A)(1) (noting plaintiffs in *Revitch* alleged that Moosejaw installed code on their devices that scanned their computers for private information, amongst various other alleged harms). Further, the *Revitch* court concluded without any discussion or analysis that plaintiffs had sufficiently pled injury by parroting the statutory requirements and "alleged injuries traceable to Moosejaw's possession and use of the device." 2019 WL 5485330, at *3.

In *Facebook III*, the Ninth Circuit observed that Sections 631 and 632 of CIPA "codif[ied] a substantive right to privacy, the violation of which gives rise to a concrete injury sufficient to confer standing." 956 F.3d at 598. However, Plaintiffs present no other case besides *Revitch* that has ever held that mere possession of a wiretapping device pursuant to Section 635 of CIPA meets this concrete injury requirement. With good reason: the "core provisions of [CIPA] regard[] interception and use of private communications." *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1118 (9th Cir. 2020). There is no basis to find that mere possession of an alleged eavesdropping device, without more, violates one's privacy rights. Interpreting the statute to permit such claims would be "constitutionally problematic." *Cohen v. Casper Sleep Inc.*, 2018 WL 3392877, at *5 (S.D.N.Y. July 12, 2018); *see also In re Lenovo*, 2016 WL 6277245, at *7 (finding that possession of a device alone cannot be sufficient to justify Wiretap Act standing).

Indeed, Plaintiffs' own authorities support Noom's position. In *Luis v. Zang*, the court denied a motion to dismiss where the defendant allegedly violated the federal Wiretap Act "by manufacturing, marketing, and selling a violative device." 833 F.3d 619, 637 (6th Cir. 2016). In so holding, it observed that "our narrow holding. . . . does not support a cause of action against those who simply possess a wiretapping device." *Id.* According to the *Luis* court, a private suit could only proceed where the defendant played "an active role in the use of the relevant device." *Id.* Plaintiffs' bare allegations of Noom's "partnership" with FullStory plainly do not suffice.[4]

Finally, Plaintiffs' proposed interpretation of Section 635 also fails because it would render this provision redundant with Sections 631 and 632, given that, in order to allegedly eavesdrop or

[4] *Romero v. Securus Techs., Inc.*, 216 F. Supp. 3d 1078, 1088 (S.D. Cal. 2016) is inapposite because it involved Section 636 eavesdropping claims, rather than Section 635 claims. (Opp. at 9.)

wiretap (and thus violate Sections 631 or 632), one must possess the alleged eavesdropping/ wiretapping device (Section 635). The holding in *Luis* that mere "possession" of a wiretapping device is not itself a wiretapping violation is therefore in accord with the "cardinal rule of statutory interpretation that no provision should be construed to be entirely redundant." *Republic of Ecuador v. Mackay*, 742 F.3d 860, 864 (9th Cir. 2014) (citation omitted).

4. Plaintiffs Fail to Plead that FullStory's Technology Is a Device "Primarily or Exclusively Designed or Intended for Eavesdropping."

Plaintiffs claim they have plausibly alleged FullStory's code was "primarily or exclusively" designed for eavesdropping, pointing to a single sentence in their FAC in which they allege that the code "is designed to gather PII, including keystrokes, mouse clicks and other electronic communications." (Mot. at 9-11; FAC ¶ 81.) But this bald allegation about the type of information collected is insufficient to allege that the code is intended for ***eavesdropping***, as required by the statute. *Cf. Luis*, 833 F.3d at 634 (denying motion to dismiss federal wiretap possession claim where defendant marketed the device "as a means for one spouse to illegally monitor the communications of another spouse"). Plaintiffs' own description of FullStory as a SaaS provider that is used to help businesses improve their websites contradict their allegation that FullStory's service is primarily or exclusively used for eavesdropping. (FAC ¶¶ 11, 18.)

Plaintiffs once again rely almost exclusively on *Revitch* in their opposition.[5] But *Revitch* merely concludes without any analysis that "the Court must assume the truth of Revitch's allegation that NaviStone's code is a 'device . . . primarily or exclusively designed or intended for eavesdropping.'" *Revitch*, 2019 WL 5484330, at *3 (quoting § 635).). That reasoning is contrary to *Iqbal*, which holds that courts need not accept as true "threadbare recitals of a cause of action's elements, supported by mere conclusory statements." *Ashcroft v. Iqbal*, 556 U.S. 662 (2009). The *Revitch* court should not have credited those plaintiffs' mere regurgitation of the statutory requirements, and this Court should not duplicate its flawed holding.[6]

[5] Plaintiffs also cite *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051 (N.D. Cal. 2015), but that case is irrelevant. There, the court addressed whether transitory storage constitutes a real-time transmission as required by CIPA, an argument that Noom does not make in its Motion. (Opp. at 11.)

[6] FullStory's code is used in a manner identical to any technology designed to facilitate web-browsing activity, including cookie technology. In a recent *Revitch* filing, the same Plaintiffs'

B. Plaintiffs Fail to Allege an Invasion of Privacy.

Plaintiffs baselessly claim that it would be "reversible error" for this Court to find that they have failed to plead a violation of their constitutional right to privacy. (FAC ¶ 2.) Plaintiffs do not dispute that ***Noom*** was entitled to receive any information they voluntarily provided. Instead they posit that Noom induced a violation of their right to privacy by permitting its SaaS provider to collect this information on Noom's behalf. (Opp. at 11-16.) Plaintiffs fail to cite a single case to support their novel theory or allege any actual or potential injury from Noom's alleged collection of their routine browsing information. This is hardly a violation of their privacy rights "so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009) (internal quotation marks and citation omitted). Plaintiffs do not come close to meeting any of the three elements of pleading a violation of the right to privacy under California law, and their claims therefore should be dismissed. *See, e.g.*, *Moreno v. S.F. Bay Area Rapid Transit Dist.*, 2017 WL 6387764, at *8 (N.D. Cal. Dec. 14, 2017); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1041 (N.D. Cal. 2014).

1. Plaintiffs Do Not Have a Legally Protected Privacy Interest.

Plaintiffs misleadingly claim that "Noom ask[s] this Court to determine as a matter of law, upon the pleadings and without a developed factual record, that PII and PHI—including health, dieting, and medical information—cannot ever legally constitute 'information subject to constitutional protection.'" (Opp. at 11 (citing Mot. at 13).) Not so. Noom's Motion asks the Court to hold that Plaintiffs' allegations ***in this case*** have failed to establish either of the two classes of legally protected privacy interests—"autonomy privacy or information privacy."[7]

---

counsel effectively conceded the similarities between pervasive technologies such as Google Analytics, which counsel suggested was not in violation of CIPA, and the FullStory technology as alleged in the FAC. In distinguishing Google Analytics and the specific technology at issue in that case, plaintiff's expert pointed to, *inter alia*, "the purpose for which the data are collected . . . the parties to whom the data are made available . . . the deep integration of NaviStone's code with third-party data brokers like Neustar and Computech, and [] the real-world effects of the data collection . . . ." Pl. Reply in Supp. of Mot. for Class Certification at 1–2, *Revitch v. New Moosejaw, LLC*, No. 18-cv-06827 (N.D. Cal. Dec. 31, 2020), ECF No. 145. This juxtaposition falls apart when applied to FullStory, as Plaintiff does not and could not allege that FullStory provides the information it collects as a service provider to anyone other than Noom. (FAC ¶¶ 1, 11–12, 18.)

[7] Plaintiffs' passing reference to *In re Vizio* does not further their cause. *In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1232 (C.D. Cal. 2017) (Opp. at 12 n.9.). There, the Court held that Plaintiffs plausibly alleged invasion of privacy based on the defendants "collect[ion] [of] an

As to autonomy privacy, Plaintiffs cite no cases applying bodily autonomy to any information potentially at issue here—*i.e.*, weight loss information input on a website. Autonomy privacy is akin to bodily autonomy (such as a right to obtain an abortion or to not provide urine for a drug test) and courts have not found "cause to extend the bodily autonomy line of cases to data autonomy." *In re Google Location Hist. Litig.*, 428 F. Supp. 3d 185, 198 (N.D. Cal. 2019).

As to informational privacy, Plaintiffs generally claim that "[c]urrent privacy expectations are developing," (Opp. at 12 (citing *McDonald v. Kiloo ApS*, 2019 WL2211316, at *4 (N.D. Cal. May 22, 2019)), yet offer no authority or logic that would support their bid to extend California privacy law to information voluntarily disclosed to a website (or collected on the website's behalf to improve website function). *See In re Google Location History Litig.*, 428 F. Supp. 3d at 198 (dismissing informational privacy claims where (as here) defendants "only tracked and collected data during use of [defendant's] services."); *In re Google, Inc. Priv. Pol'y Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014) (dismissing informational privacy claims based on commingling of user data across Google products and disclosing that data to app developers).

Plaintiffs' informational privacy claims also fail because they do not allege, as they must, that their information was "disseminated or misused" in any fashion. (FAC ¶ 2.) *Alch v. Superior Ct.*, 165 Cal. App. 4th 1412, 1423 (2008) ("Informational privacy. . . . is the interest 'in precluding the dissemination or misuse of sensitive and confidential information.'") (citation omitted). While Plaintiffs claim that they have pled "dissemination" because the data was shared with FullStory, nowhere do they allege that any data was disseminated beyond Noom's service provider or that FullStory could even potentially misuse any information that was purportedly collected. (Mot. at 12.) To the contrary, Plaintiffs only allege the information was shared with FullStory as Noom's service provider to be used only for Noom's purposes. These allegations do not satisfy the "dissemination" or "misuse" requirement.

---

exceptionally vast array of information about [plaintiffs'] digital identities and [video] viewing histor[ies]" including where customers believed they have opted out of such practices. *Id.* at 1233. Based on "the quantum and nature of the information collected, the purported failure to respect consumers' privacy choices, and the divergence from the standard industry practice," the court concluded that plaintiffs plausibly alleged an invasion of privacy. *Id.* No such facts are pled here. *Supra* section I.

2. Plaintiffs Do Not Have a Reasonable Expectation of Privacy.

Plaintiffs plead that they voluntarily transmitted information to Noom and concede in their Opposition that they had no expectation that their communications would be kept private from Noom. (Opp. at 12-13.) Nevertheless, they claim that Noom violated their subjective expectation that the information they voluntarily disclosed to Noom would be kept confidential even from Noom's service providers. The two cases Plaintiffs cite, however, involved instances where the defendants were not parties to the underlying communications and allegedly made various representations that led plaintiffs to reasonably believe those communications would not be collected. In *Facebook III*, the defendant was not the intended recipient of GET requests between plaintiffs and other websites, and nevertheless surreptitiously collected this information to develop its own "cradle-to-grave" profiles of the users. 956 F.3d at 599, 603. (Mot. at 17.) The Court held that plaintiffs plausibly alleged a reasonable expectation of privacy based on Facebook's representations, which "set an expectation that logged-out user data would not be collected, but then collected it anyways." 956 F.3d at 602. Likewise, in *In re Google Location History Litig.*, plaintiffs alleged a reasonable expectation of privacy based on concrete allegations that Google contradicted its own representations to users by "collect[ing] and stor[ing] users' location data even when their Location History was set to off." --- F.Supp.3d ----, 2021 WL 519380, at *1 (N.D. Cal. Jan. 25, 2021). Here, in contrast, Noom explicitly discloses to Plaintiffs in its privacy policy that data regarding their interactions with the website may be collected by Noom ***and by Noom's service providers***.[8] (ECF No. 35 at 14-15 (FullStory's Mot.).)

Besides the lack of apposite case law, Plaintiffs' claims fail because a reasonable expectation of privacy must be based on "an objective entitlement founded on broadly based and widely accepted community norms." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 37 (1994). Plaintiffs' subjective and unreasonable suspicion that Noom would contradict its own privacy policy and keep information from its service providers does not meet this objective standard.

3. Noom's Conduct Is Not Highly Offensive to a Reasonable Person.

[8] *See* https://web.noom.com/ terms-and-conditions-of-use/noom-privacy-policy (last modified Dec. 17, 2018).

Finally, Plaintiffs attempt to avoid dismissal of their privacy claims by arguing that Noom's conduct was "highly offensive." Plaintiffs base their position on claims that (1) there is "no bright line on offensiveness" and this case presents factual issues that cannot be decided on a motion to dismiss; and (2) the Court should ignore California Court of Appeals precedent that routine commercial collection of information is not highly offensive. Neither argument is persuasive.

To start, Plaintiffs incorrectly contend that the question of whether "Noom's conduct [is] sufficiently offensive raises a question of fact." (Opp. at 14.) Even assuming the facts pled here to be true, courts routinely dismiss privacy claims based on far more egregious facts because privacy claims must withstand an "extraordinarily high bar." (Mot. at 15-16 (citing, *e.g.*, *In re Google Android Consumer Priv. Litig.*, 2013 WL 1283236, at *2, *9–11 (N.D. Cal. Mar. 26, 2013) (dismissing claims based on allegations of tracking and sharing of "highly detailed and confidential [PII] over a substantial period of time without [Plaintiffs'] knowledge or consent")).)

The handful of courts that have denied dismissal of such claims have done so on facts that are readily distinguishable—*i.e.*, systematically using cell phone GPS data to "continually . . . log [] precisely where [plaintiffs] live, work, park, dine, pick up children from school, worship, vote, and assemble" and then sell that data, *Goodman v. HTC Am., Inc.*, 2012 WL 2412070, at *14 (W.D. Wash. June 26, 2012) (internal quotation marks omitted); or surreptitious collection of "private browsing mode" browser history, including "a user's dating history, a user's sexual interests and/or orientation, a user's political or religious views" *Brown v. Google LLC*, --- F.Supp.3d ----, 2021 WL 949372, at *21 (N.D. Cal. Mar. 12, 2021). No such facts are pled here.

Further, Plaintiffs attempt to distinguish *Fogelstrom*, cited in Noom's Motion, by arguing that the case did not involve "'surreptitious' acquisition of personal information." (Opp. at 21.) Plaintiffs are wrong. *Fogelstrom* involved collection of information used to identify home addresses, and "Courts have frequently recognized that individuals have a substantial interest in the privacy of their home." *Fogelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 990 (2011); *Cnty. of L.A. v. L.A. Cnty. Emp. Rels. Comm'n*, 56 Cal. 4th 905, 927 (2013). As here, the court in *Fogelstrom* held there was no privacy claim because the plaintiffs failed to allege the defendants used that information "for an offensive or improper purpose" rather than for "routine commercial

behavior." *Fogelstrom*, 195 Cal. App. 4th at 992-93.

Plaintiffs invite the Court to ignore *Fogelstrom* and instead apply *Opperman v. Path I and II*. These cases are inapposite. *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018 (N.D. Cal. 2014); *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1079 (N.D. Cal. 2016). Plaintiffs there alleged that defendants copied users' entire iPhone address book without their consent, and that this practice thereby left "[plaintiffs'] private information vulnerable to unauthorized download" by third parties. *Opperman*, 87 F. Supp. 3d at 1032-33. No such facts are pled here. Even if these cases were similar, Judge Tigar even acknowledged *Opperman* to be a novel interpretation of the case law, which generally finds commercial collection of customer data is not highly offensive. *See Opperman*, 205 F. Supp. 3d at 1077-78 (N.D. Cal. 2016) (listing contrasting decisions).

III. PLAINTIFF MOISE FAILS TO PLEAD INJUNCTIVE RELIEF.

Plaintiff Graham has abandoned her claim for injunctive relief. Plaintiff Moise argues she has standing to pursue this claim because it is "reasonably inferred" that she is imminently likely to suffer future injury absent an injunction. *City of L.A. v. Lyons*, 461 U.S. 95, 111 (1983). Yet the only allegation of future harm in the FAC relates to Plaintiffs "continue[ed] desire to use the internet" in a manner that is not "monitored or recorded" by FullStory. (FAC ¶ 75.) These allegations of speculative future injury are not specific to Noom and therefore cannot support injunctive relief. Further, Plaintiff Moise claims she never signed up to use Noom and makes no claims about her intent to visit Noom's website in the future. (FAC ¶ 5.) On this basis, Plaintiff Moise's only authority is easily distinguishable. *See Davidson v. Kimberly-Clark Corp.*, 889 F.3d 956, 970-71 (9th Cir. 2018) (finding plaintiff alleged likelihood of future harm based on desire to purchase product again; her "regular visits" to stores where such products were sold; and the fact that she was "continually presented with [the product] packaging but has 'no way of determining whether the representation . . . is in fact true'").

IV. CONCLUSION.

For these reasons, this Court should grant the Motion and dismiss all claims with prejudice.

Dated: March 19, 2021

COOLEY LLLP

By: */s/ Michael G. Rhodes*
Michael G. Rhodes

Attorneys for Defendant
Noom, Inc.

246525813